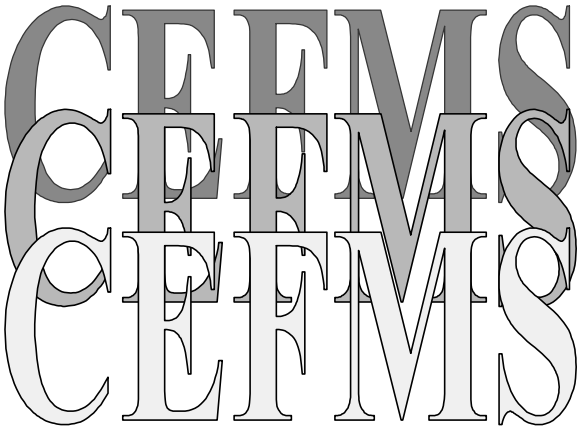
US Army Corps
of Engineers

Electronic Signature Users Guide

Version 3.0

September 15, 2003



Corps of Engineers Financial Management System

Electronic Signature
Users Guide

Version 3.0

FOREWORD

The CEFMS Electronic Signature (Esig) capability is limited to valid CEFMS users who have been granted authorization in the Access Control Table. To perform these capabilities, an individual must be assigned a **smartcard**. There are grave responsibilities that come with the issuance and receipt of smartcards. Refer to Appendix A of this document for a list of smartcard holder's responsibilities, along with signature requirements acknowledging that as a smartcard holder you have read and understand these responsibilities. Appendix B provides similar signature requirements for smartcard approvers. Appendix C provides District Security Officer (dSO) Operating Procedures. Appendix D provides an Overview of Card Assignment Rules. **Refer to paragraph 2.6 of this document for procedures necessary to dispose of Esig boards.**

ELECTRONIC SIGNATURE USERS GUIDE

TABLE OF CONTENTS

ELECTRONIC SIGNATURE USERS GUIDE

TABLE OF CONTENTS

PAGE

LIST OF FIGURES

APPENDICES

Security of the Smartcard and Pin

Memorize your Pin. Do Not write it down or share with others. Report a lost, stolen or compromised card to your dso immediately. ***REF AR 380-19, Information Systems Security, paragraph 2-14, Password Control****.*

SECTION 1.0 GENERAL

1.1 Introduction.

The Corps of Engineers Financial Management System (CEFMS) provides the capability to electronically sign documents. The electronic signature generated by the system is a replacement for a handwritten signature. An electronic signature will provide assurance that a document was signed by an authorized person and that the document was not altered after it was signed. Hardcopy documents can be altered without detection and handwritten signatures can be forged. With electronic signatures, these alterations will be detected. Electronic Signatures will reduce the amount of paper that must be routed. Documents can be reviewed on screen and signatures verified using the Electronic Signature System (ESS). The following paragraphs provide information that a user or security administrator should have in using the system.

1.2 Definitions.

The following terms are commonly used when referring to the electronic signature system.

1.2.1 ARGUS 300 Adapter Board - a board installed in a PC which performs the functions of the electronic signature system.

1.2.2 CEFMS Database Administrator (DBA) - an individual providing technical support, including enforcing the policies and standards set by the data administrator for the database. In addition to providing maintenance, the DBA coordinates with other computer operations technicians, system developers, vendors, and users.

1.2.3 Central Security Officer (cSO) - a person at a regional center responsible for maintaining the Key Translation Center (KTC) of the ESS. There will be two cSOs at each regional center with each having a backup.

1.2.4 Cryptographic Keys - keys that are stored on the card or generated by the PC Adapter Board and used in the electronic signature process.

1.2.5 Data Administrator (DA) - the individual responsible for the life-cycle management of the information describing the functions, operations, and structure of the organization's databases. These responsibilities include prescribing policies and standards, planning, coordinating, resolving conflicts, designing logical databases, and controlling security. The DA also ensures that life-cycle planning includes on-line retention issues as well as archival criteria and methods.

1.2.6 Database - a generalized, integrated collection of interrelated data, organized according to a plan to satisfy the data requirements of all applications which use it.

1.2.7 District Security Officer (dSO) - a person responsible for issuing smartcards, Personal Identification Numbers (PINs), and performing other Electronic Signature management functions. There are two primary dSOs designated dSO1 and dSO2. Primary dSOs have at least one (but no more than two) backup designated dSOb1 and dSOb2.

1.2.8 Electronic Signature Drivers/Software - software to interface CEFMS and other applications with the PC Adapter Board.

1.2.9 Key Translation Center (KTC) - a central database containing all the Users of the Electronic Signature System (ESS), i.e., cSOs, dSOs, SAs, and Users. This database is accessed when verifying the signature of a user. There will be two regional centers located at Vicksburg, MS and Portland, Oregon. Each will have two KTCs and will serve as backups for each other.

1.2.10 Message Authentication Code (MAC) - a combination of characters which represents the electronic signature. The MAC is generated using the data being signed and the User=s and SA=s cryptographic keys.

1.2.11 PC Adapter Board - a board installed in a PC which performs the functions of the ESS.

1.2.12 Personal Identification Number (PIN) - a randomly generated pronounceable password issued to a cSO, dSO, SA, or User which is required in order to use the ESS. Upon entering CEFMS, the application prompts the cSO, dSO, SA or User to insert their smartcard into the smartcard reader and then prompts for their PIN.

1.2.13 Security Administrator (SA) - an employee issued a card who will be responsible for initialization of a PC Adapter Board so that users can sign documents. SAs who initialize PC Adapter Boards in PCs used in the disbursing functions and the user signing the checks will be held liable for fraudulent transactions. SAs will not be held liable for fraudulent or erroneous transactions signed for by Users with signature authority for functions outside of disbursing.

1.2.14 Smartcard (card) - a card, similar in size and shape to an automated teller card or credit card. A smartcard is issued to each authorized cSO, dSO, SA, or User to gain access to the ESS. The smartcard contains a microprocessor chip that actually stores data and performs calculations. Each card has its own serial number for identification. The smartcard is commonly referred to as a signature card.

1.2.15 Smartcard Approver - a person responsible for approving an employee's request for a smartcard. The Smartcard Approver ensures the employee is authorized by the Laboratory or Support Staff Chief to obtain a smartcard. Upon verification, the request is approved and electronically sent to the dSOs.

1.2.16 Smartcard Reader - a device connected to the PC adapter board which reads data stored on the smartcard and passes it securely to the PC adapter board.

1.2.17 User - an employee issued a smartcard and responsible for signing documents. Users who electronically sign documents accept the same responsibility as when signing documents by hand.

1.3 Hardware/Software Requirements.

To electronically sign documents, a smartcard user logs onto CEFMS on a computer equipped with the Electronic Signature hardware and software. The basic computer requirements include:

- PC with AT (ISA) Bus 80286, 80386, or 80486 CPU with EGA or VGA monitor and appropriate card. **NOTE:** The Electronic Signature will not work on a Macintosh or an IBM PS/2 computer. Electronic signature may be used with a notebook computer with the Signet device.

- 640 KB RAM; but recommend at least 2.5 additional MB RAM if other software packages will be run on the user's PC.

- 300 KB hard disk storage; but recommend at least 5 MB hard disk storage if other software applications will be run on the user's PC.

- DOS 5.0 Or higher if possible.

- 1 serial port.

- 3COM 3c503 Ethernet card if on an Ethernet Lan.

- Capability to access the CEFMS database via LAN connection or modem.

- PC Adapter Board.

- Smartcard Reader.

- Electronic Signature Software.

- Activated Smartcard.

- Personal Identification Number (PIN).

SECTION 2.0 SECURITY PROCEDURES

2.1 Smartcard Security.

When receiving a card and PIN, it is very important to follow the security procedures listed below.

2.1.1 Always keep the card in a safe place when it is not being used. A wallet or a locked drawer is the best place to keep the card.

2.1.2 Sign the PIN envelope before opening to validate that it has not been tampered with prior to receipt.

2.1.3 Return the top sheet of the envelope to the dSO issuing the password.

2.1.4 Memorize the PIN then destroy the second sheet of the envelope. Do not throw it away without shredding the document first.

2.1.5 Do not write the PIN down or give it to another User.

2.1.6 If the PIN is revealed to another User, immediately contact the dSO for a new card. If the card is lost or stolen, immediately contact the dSO. The dSO will deactivate the card so that it can no longer be used. A new card and PIN will be issued.

2.1.7 A lost card or compromised PIN is a serious security issue since the User can be held responsible for transactions authorized with the missing or compromised card.

CONTACT THE dSO *IMMEDIATELY* IF A CARD IS LOST OR PIN COMPROMISED.

2.2 Deactivate Smartcard Due to Employment Termination.

Smartcards will be deactivated when a user leaves an organization. The card must be returned to the dSOs so it can be deactivated to prevent the user from signing any additional messages. The flag in the database will be set to indicate that although the user is no longer active, the signatures generated by the user may still be validated.

2.3 Compromised PIN.

Smartcards will be deactivated when a PIN is compromised or the user suspects a PIN is compromised. The smartcard must be promptly returned to the dSOs. The user is not deleted from the database so that signatures generated by the user may still be used to verify messages previously signed by the user. The user will receive a new smartcard and PIN.

2.4 Lost Smartcard.

Smartcards will be deactivated when a card is lost. The dSOs must be notified immediately that a card was lost. The database will be updated to set the flag to indicate that although the card is no longer active, the signatures previously generated by the user may still be verified. The database will be updated with the date a smartcard is deactivated. Any signature generated after this date may not be verified. The user will receive a new smartcard and PIN.

2.5 Security Violations.

2.5.1 If a user sees or knows of unauthorized use of smartcards or PINs, i.e., sharing, notify the individual's supervisor for appropriate disciplinary action.

2.5.2 If a user finds an unattended computer with a smartcard in the smartcard reader, attempt to log them off CEFMS and remove the smartcard. If the user cannot log them off, remove the smartcard and take to the individual's supervisor. Inform the supervisor of the incident so that he/she may take appropriate disciplinary action.

2.5.3 If a user finds a smartcard, take it to your supervisor so he/she may decide if disciplinary action is necessary. The user may have already reported the loss of the smartcard to a dSO.

2.5.4 If a user finds a PIN written down, notify the supervisor for appropriate disciplinary action. PINs should be memorized and not written down for unauthorized viewing.

2.6 Disposing of Esig Boards.

The Litronic ARGUS 300, ESIG Board, must be un-SAed before disposing of the board. The un-SAing process removes encryption keys from non-volatile storage on the board. The un-SA-ing process is accomplished from within CEFMS. The board must remain installed in a computer and the CEFMS application accessed before the board can be un-SAed. Once logged into CEFMS, access the <Log Off SA> option from the Electronic Signature Menu. You will be requested to insert an SA card to be logged off. Any SA card can be used. Type in the PIN of the SA card that you are using for the un-SA process. To verify the SA is logged off after completing the un-SA process, remove the SA card. Select the <Log Off SA> option again. If nothing happens, the board was successfully un-SAed. ***NOTE:*** *Cutting the leads from the battery on a defective Esig board will insure the removal of encryption keys from non-volatile storage (suggestion).*

SECTION 3.0 OPERATING PROCEDURES

3.1 Requesting a Smartcard.

Requests for a smartcard and PIN must be made through CEFMS. The request is approved by an authorized person, who then forwards the request to the dSOs. The dSOs assign a card and then issue the card and PIN to the requestor.

3.1.1 To request a smartcard, a valid CEFMS user ID and password are required. After receiving a userid and password, follow the steps listed below in order to request and receive a smartcard:

- Login to the system where the CEFMS database resides.
- Enter the command to execute CEFMS.
- From the CEFMS Main Menu, select option 7 - **ELECTRONIC SIGNATURE FUNCTIONS.**
- From the Electronic Signature Menu, select option 3 - **REQUEST SMARTCARDS.** This option will display screen 15.1, Request Electronic Signature Smartcard.
- Press **<F9>** to request card and then enter the card type: **U** for User Card, **S** for Security Administrator Card, **D** for Security Officer Card.
- **<PgDn>** to view the request information and check the request status.

3.1.2 A user may only make one request at a time. If a user has a smartcard, that card must be deactivated by the dSOs before another card request can be made.

3.1.3 The request will be electronically forwarded to a Smartcard Approver, who must electronically approve the request before a smartcard can be issued. Reference Appendix B for Smartcard Approvers duties.

3.1.4 Once the request is approved, the dSOs will assign a smartcard. A dSO will notify the requestor as to when and where the card and PIN can be obtained. If the card and PIN is to be received in person, the dSOs will activate the smartcard and present the smartcard and PIN envelope to the user. The user must then sign and date the PIN envelope and leave the header sheet with the dSOs. (If the requestor is at a remote site, a dSO will mail the PIN envelope first. The smartcard will not be activated and mailed until the PIN envelope is signed and the header sheet returned to the dSOs.)

3.2 Issuing of Smartcards.

If a user appears in person to receive a smartcard:

3.2.1 A valid driver license or Civilian ID card may be required to verify identification.

3.2.2 The individual will be given a copy of the Electronic Signature Users Guide. The user must read, sign, and date the Smartcard Holders Responsibilities Form before receiving a smartcard and PIN. A copy of the signed signature page will be provided to the user.

3.2.3 After verifying the person's identity, the dSOs will activate the smartcard and issue the smartcard and PIN to the employee.

- If the smartcard being issued is for a User, dSO1 will issue the smartcard and dSO2 will issue the User PIN envelope.

- If the smartcard being issued is for a SA, dSO2 will issue the smartcard and dSO1 will issue the SA PIN envelope.

3.2.4 The individual will check the PIN envelope to detect tampering. If none is found, the user will sign the top portion of the envelope, tear it off, and return to the issuing dSO. The dSO will file the signed top portion.

3.2.5 The bottom portion containing the smartcard holder's unique PIN (i.e., password) is kept by the individual.

3.3 Remote Assignment and Issuing of Smartcards.

If a user is remotely located and cannot receive his/her card in person:

3.3.1 If the smartcard request is approved by the Smartcard Approver, the dSOs will assign a smartcard through the DSO CARD ASSIGNMENT SCREEN.

3.3.2 The requestor will be mailed the smartcard by **Certified Mail - Return Receipt Requested**.

3.3.3 When a user receives the smartcard, he must sign for the Certified Mail and call the issuing dSO to acknowledge receipt of the smartcard. If a user does not receive the smartcard in a reasonable amount of time or if the smartcard is damaged, notify the dSO so that appropriate action can be taken.

3.3.4 Upon confirmation of having received the smartcard, the dSO will mail the PIN envelope by **Certified Mail - Return Receipt Requested**.

3.3.5 When received, sign for the mail. Examine the PIN envelope for tampering. If okay, sign the top portion of the PIN envelope and tear it open. The bottom portion contains the PIN and serial number of the assigned card. **Memorize the PIN and destroy the bottom portion** of the envelope by shredding or burning. Any hard copy of a PIN must be kept in the user's physical possession or secured in a locked cabinet, drawer, or container accessible only by the user.

3.3.6 Return the top portion of the PIN envelope to the issuing dSO by **U.S. Postal Service - Regular Mail, First Class**.

3.3.7 Call the issuing dSO to acknowledge receipt of the PIN envelope.

3.3.8 Upon confirmation of the user having received the PIN envelope, the appropriate dSO will activate the smartcard.

3.4 Expiration of Smartcards.

All user and SA cards will expire within three years from the date of activation except users performing disbursing and dSO functions; and those cards will expire in one (1) year. The one (1) year expiration occurs when the Access Control authorization for receipt voucher audit (rv_audit_ind) or receipt voucher certification (rv_cert_ind) or disbursing authority (disb_auth) or disbursing officer (disb_officer_ind) or district security officer (dist_sec_ofcr_ind) or travel settlement authority (trv_setl_auth_ind) = 'Y'. Users will be given the first warning message 30 days before the card will expire. The user may request a new card even though the current card is not deactivated. However, the old card must be turned in before the dSOs can activate the new card. **REQUEST A NEW CARD AS SOON AS** the warning message is given! Expired cards cannot access the ESS.

3.5 General Operating Procedures.

3.5.1 The card types are designed for either a User or a Security Administrator (SA). A SA can also be a User; but a User cannot be the designated SA and user on a PC at the same time.

3.5.2 The SA must initialize the PC adapter board to be used for electronic signatures. After the SA has initialized the board, any number of Users can use the Electronic Signature System to sign documents.

3.5.3 Cards must be inserted into the card reader correctly. The LITRONIC logo should face **down**. With thumb on the arrow, insert into the card reader.

3.5.4 CEFMS will then prompt for a PIN. When entering a PIN, the CAPS LOCK key should be **off**. The PIN will be in **lower case.**

3.6 Security Administrator (SA) Operating Procedures.

3.6.1 If a board has not been previously initialized by a SA, a screen will appear when entering CEFMS which prompts the SA to enter the card and then the PIN.

3.6.2 The SA will be given four tries to enter the correct PIN after which CEFMS will log you out. After nine consecutive incorrect PINs, the card will be locked and the dSO will have to unlock the card.

3.7 Esig SA Management Tools.

There are two programs that provide SA management tools: LISTSA2 and GETSA. LISTSA2 (located on user's UNIX machine at unix/usr/tools/cefms/bin/listsa2 yourfilename.txt.

Purpose: A program that allows a user to enter an SA's card serial number and get a list of users that have been SA'd by the user executing the program. The program will list all users who have logged on to a PC SA'd by that card.

Execution:

- Connect to UNIX and at the UNIX prompt, type the program name followed by a file name (unix>listsa2 yourfilename.txt) where yourfilename is the file where the program output will reside.
- The program will begin and the user will be prompted to enter a SA serial number. (This will list the users associated with the SA Card. These records are listed on the screen and written to the file above.)
- To exit the program, press <Enter> when prompted for a serial number. NOTE: If a user is executing Esig by SA card number, transactions on a machine other than their own, their info will show up under whoever SA'd the PC being used. The file will only contain the data since the last time it was run.

GETSA (located on your UNIX machine at unix> /usr/tools/cefms/bin/getsa yourfilename.txt.

Purpose: A program that allows a user to list what SA Card/User has SA'd a PC.

Execution:

- Log into CEFMS on the PC that should identify the card/user that SA'd the PC - before executing GETSA.
- Connect to UNIX and at the UNIX prompt, type the program name (unix>getsa) and press <Enter> to execute the program.

3.8 User Operating Procedures.

Once the SA has initialized the PC Adapter Board, the User will be prompted to insert the card and enter the PIN. The User will follow the procedure in **paragraphs 3.3.3** and **3.3.4**. The User will be given four tries to enter the correct PIN after which CEFMS will log the user out. After nine consecutive incorrect PINs, the card will be locked.

3.8.1 After a successful log on, do not remove the card until exiting from CEFMS. If the card is removed before exiting CEFMS, the card will be locked. Users may unlock their own card when logging back into CEFMS.

3.8.2 When entering CEFMS, several errors may occur that will prevent the User from using the electronic signature capability. If errors occur while using the electronic signature capability, write down the error code and contact the site's CEFMS POC for resolution of the problem.

3.8.3 If a signature does not verify on a document, a message will appear on the screen. This indicates that the document has been altered in some way and the alteration must be resolved in order to continue. Contact the originator of the document or the site's CEFMS point of contact to resolve the problem.

3.8.4 After entering CEFMS, an error message may appear during the verification or signing of a document. If an error occurs, write down the error code that appeared and contact the site's CEFMS POC for resolution of the problem.

3.9 District Security Officer (dSO) Operating Procedures.

Reference Appendix C for the functions, responsibilities, and operating procedures of the dSO.

3.10 Access Control Functions Which Require Electronic Signature.

Electronic Signature will be the means used to identify the authenticator of information and to verify that critical data on a document has not been altered. The only required users of Electronic Signature are those who perform level III security functions, i.e., those where actions/approvals lead to an obligation, collection, or disbursement of government funds.

3.10.1 The immediate supervisor of each employee requiring access to the CEFMS database may be tasked to submit the Request For CEFMS Access Form. This form will be submitted to the CEFMS DataBase Administrator. The functions checked on the form provide information for the CEFMS DBA to grant the user access and authorization to control the activities they will be able to perform, including the need for electronic signature capability. Figure 3-1 depicts a sample CEFMS Access Form.

3.10.2 The CEFMS DBA will ensure that the appropriate Smartcard Approver receives the names of individuals needing a smartcard based on authorizations granted in the CEFMS Access Control Table. An asterisk indicates those authorizations which require electronic signature capability. To obtain a more detailed understanding of the functions capabilities which are assigned through the CEFMS Access Control Table, reference the CEFMS Access Control (Authorizations Cross Referenced To Functionalities) document.

3.11 Card Assignment Rules.

Reference Appendix D of this document for an overview of card assignment rules.

REQUEST FOR CEFMS ACCESS FORM

NAME: _____ **USERID:**_____ **PHONE:** _____

SUPERVISOR'S APPROVAL: _____ **DATE:** _____/_____/_____

Check The Desired Access (*Requires Esig Capability):

|*| ACCPT CUST ORD
|_| ACCRUAL AUTHORITY
|_| ACPERS
|_| ADJUST WAREHOUSE INVENTORY
|_| AGENCY RATE AUTHORITY
|_| APPROP EXP AUTHORITY REQUEST
|_| APPROP EXP AUTHORITY APPROVAL
|_| APPROVE ADJUST WAREHOUSE INVENTORY
|*| APRV PR&C
|_| ASSET BATCH IND
|_| ASSET MANAGER AUTHORITY
|*| AUTHORIZED COLLECTOR
|_| AUTHORIZED PROPERTY OFFICER
|*| AUTHORIZED RECEIVER
|_| BUDGET APPROVAL AUTHORITY
|_| BUDGET FORMULATION LEVEL
|*| CERT PR&C
|*| CERTIFY GOV'T TRAINING BILLS AUTH
|*| CERTIFY TRAINING TFO's AUTHORITY
|*| COMMERCIAL TRANSPORTATION AUTH
|*| CONVERSION AUTHORITY
|_| COST SHARE CONTROL IND
|_| COST SHARE ESCROW/LOC AUTH
|_| COST SHARE RECORD EARNINGS IND
|_| COST SHARE RECORD IN-KIND IND
|_| COST TRANSFER
|_| CUPBOARD STOCK TRANSFER IND
|_| CUSTOMER ORDER ROLLOVERS
|_| DATA MGR ESIG FAIL RESOLUTION AUTH IND
|*| DISBURSING AUTHORIZATION
|*| DISBURSING/DEPUTY DISBURSING OFFICER
|*| DISBURSING SCRTY ADMIN AUTH
|*| DISTRICT SECURITY OFFICER
|_| ELECTRONIC FUNDS TRANSFER AUTH IND
|*| ENG 93 C.O.R. APPRV
|*| ENG 93 P.M. APPRV
|*| FINAN APRV
|_| FOREIGN CURRENCY REVALUATION AUTH IND
|*| FUND OVRD
|_| FUNDING ACCOUNT IND
|_| FUNDING ACCOUNT OVERHEAD IND
|_| FUNDING CREATOR
|_| GENERAL LEDGER JOURNAL AUTHORITY
|_| GENERATE CUSTOMER ORDER BILLS
|_| GENERATE FACILITY BILLINGS
|_| GENERATE INVENTORY BILLINGS
|_| GENERATE PLANT RENTAL BILLINGS
|*| GOVERNMENT ORDER ACCEPTOR
|_| IATS INTERFACE AUTHORITY
|*| IMPREST FUND CASHIER
|_| INCOME TRNS IND
|_| INTRA CORPS TRANSFER AUTHORITY
|*| INVOICE CREATOR
|_| JOB ORDER FUNDING CREATOR
|_| LABOR CERTIFICATION AUTHORITY
|_| LABOR DISTRIBUTION AUTHORITY
|_| LEDGER POSTING AUTH
|_| MULTI-PURPOSE POWER AUTH IND
|*| OBLIGATE TRAINING REQUEST AUTHORITY
|*| OBLIGATION APPROVER
|_| ORGANIZATION RATE AUTHORITY
|_| ORIG PR&C
|*| OTHER PURCHASES APPROVER IND
|*| OTHER PURCHASES CERTIFIER IND
|*| OTHER PURCHASES OBLIGATOR IND
|*| PCS TRAVEL AUTHORITY
|_| PERIOD CONTROL
|_| PLANT RENTAL RATE AUTHORITY
|_| PLO
|_| PRC AUTHORIZED ASSIGNER
|_| PROCESS LONG TERM REVENUE
|*| PROCESS RECEIPT VOUCHER
|*| PROCESS TRANS. BY OTHERS (TBO's)
|*| RECEIPT VOUCHER AUDITOR
|*| RECEIPT VOUCHER CERTIFIER
|_| RELEASE OF CLAIMS AUTHORITY
|_| REORG AUTH IND
|_| REPORT ACCESS LEVEL
|_| REPORT SUBMISSION IND
|_| REPORT VIEW LEVEL
|_| RESOURCE PLANS/ESTIMATES APPROVER
|_| REVENUE GENERATING AGREEMENT MAIL CODE
|_| REVERSE ACCRUALS AUTH
|_| S&A COST TRANSFER IND
|_| S&A MEMO PLACEMENT AUTH IND
|*| S&A OBLIGATION AUTH
|_| S&A PROCESS AUTHORITY
|_| S&A TRANSFER TO UFC IND
|_| SAACONS INTERFACE AUTH IND
|_| SHOP/FACILITY RATE AUTHORITY
|*| SMARTCARD REQUEST APPRV
|_| SPECIFIC EXPENDITURE AUTHORITY IND
|*| SUPERVISOR
|_| TECH APRV
|_| TIMEKEEPER
|_| TRAINING REQUEST APPROVAL AUTHORITY
|*| TRAV VOUCHER/L.D. PHONE REVIEWER AUTH
|*| TRAVEL ADVANCE AUTH IND
|_| TRAVEL APPROVING OFFICIAL
|*| TRAVEL AUTHENTICATING OFFICIAL
|_| TRAVEL REQUESTING OFFICIAL
|*| TRAVEL SETTLEMENT CERTIFY IND
|_| TRAVEL SETTLEMENT CREATE IND
|_| TRAVELERS CHECKS AUTH IND
|_| USER STATUS
|*| VENDOR APPROVAL AUTHORITY
|_| WAREHOUSE BURDEN RATE AUTHORITY
|_| WAREHOUSE STOCK RECORD AUTHORITY
|_| YEAR END CLOSINGS IND

Figure 3-1

3.12 Error Messages.

3.12.1 When entering CEFMS, several errors may occur that will prevent a smartcard holder from using the Electronic Signature capability. The user will be able to continue, but will not be able to verify any signatures electronically or electronically "sign" a document. If an error occurs, write down the error code and contact your site's CEFMS POC.

3.12.2 The following is a general list of error codes and messages to aid in the diagnosis of error conditions.

ERROR CODE	EXPLANATION OF ERROR
-11	System write() call failed
-10	System read() call failed
-9	System gethostbyname() or gethostname() call failed
-8	System accept() call failed
-7	System listen() call failed
-6	System getsockname() call failed
-5	System bind() call failed
-4	System connect() call failed. Usually means KTC is down, or KTC entries in KTC_ORACLE_SID table are bogus. Could *possibly* mean logger is down, but probably is KTC related.
-3	System socket() call failed. Usually means logger isn't working, or KTC is down.
-2	Invalid host specified
0	Success; No error
1	Side server received unknown MAC type
2	Side server received data in invalid format
3-23	Critical Argus hardware or smartcard error
24	Incorrect smartcard password (PIN) entered
25	Smartcard key in use. Un-SA board, and re-SA to fix.
26-41	Critical Argus hardware or smartcard error
42	Same user logged in twice – ie, the user SA'd himself. Un-SA machine, and re-SA with a different card to fix.

NOTE: Error numbers 1-63 are usually hardware errors. If a smartcard works on one computer with an Argus board and card reader, and it will not work on another computer with a different Argus board and card reader, in all probability, the Argus board and/or card reader is/are defective and should be replaced on the computer where the smartcard will not work. If replacing the Argus board and card reader does not fix the problem, there may be a motherboard problem. Litronic is the electronic signature hardware vendor and should be contacted concerning hardware problems. However, if using a Signet box, the vendor is Gradkell Systems.

ERROR CODE	EXPLANATION OF ERROR
43-47	Critical Argus hardware or smartcard error
48	Argus board cannot read serial number from smartcard. Generally, the smartcard is in the reader upside down or the gold contacts are dirty (they can be cleaned with an eraser). Try the card on other machines, and try other cards on this machine to get a feel for whether the problem is the card or the reader.
49-63	Critical Argus hardware or smartcard error
64	User voluntarily terminated logon by pressing cancel. If user didn't actually do this, the keyboard intercept cable is most likely hooked up improperly.
65	SA voluntarily terminated logon by pressing cancel. If SA didn't actually do this, the keyboard intercept cable is most likely hooked up improperly.
66	User pressed cancel at smartcard logoff prompt
67	SA pressed cancel at smartcard logoff prompt
68	dSO1 voluntarily terminated logon by pressing cancel. If dSO1 didn't actually do this, the keyboard intercept cable is most likely hooked up improperly.
69	dSO1 pressed cancel at smartcard logoff prompt
70	dSO2 voluntarily terminated logon by pressing cancel. If dSO2 didn't actually do this, the keyboard intercept cable is most likely hooked up improperly.
71	dSO2 pressed cancel at smartcard logoff prompt
72	No KTC information found in KTC_ORACLE_SID
73	Cryptographic module setup failed
74	Data integrity failed. The data being verified is different from the data originally signed. If this is suddenly widespread (ie everyone is getting it) there's most likely a problem at the KTC.
75	Can't read smartcard serial number
76	Can't talk to KTC
77	User cancelled smartcard remove
78	Invalid operation
79	User's card is locked, and may require the dSOs to unlock it
80	Can't get address

NOTE: Error numbers 1-63 are usually hardware errors. If a smartcard works on one computer with an Argus board and card reader, and it will not work on another computer with a different Argus board and card reader, in all probability, the Argus board and/or card reader is/are defective and should be replaced on the computer where the smartcard will not work. If replacing the Argus board and card reader does not fix the problem, there may be a motherboard problem. Litronic is the electronic signature hardware vendor and should be contacted concerning hardware problems. However, if using a Signet box, the vendor is Gradkell Systems.

81	CEFMS checked both registries for the user trying to enter CEFMS, and that user was not found. Have the user register. If problem still exists, user most likely incorrectly registered their card with the wrong CEAP ID, and CEFMS support needs to be contacted to fix.
82	File transfer program couldn't find any files to transfer
83	Grant denied by user.
84	File transfer program aborted
85	Send of files cancelled
86	Receive of files cancelled
87	Can't print
88	User cancelled print operation
89	User cancelled resolver operation
90	Can't run resolver / can't resolve failure
91	The logger isn't working properly, it's unable to log esig messages. Most likely, the tablespace / extents are full. Contact CEFMS support for resolution.
92	CEFMS cannot find WinSig listening at user's registered address. Make sure user is registered properly. Make sure WinSig is running on user's PC. If both the previous are true, a firewall is most likely blocking ports 2400-2407 somewhere between the CEAP host and the user's PC.
93	IATS upload cancelled
94	IATS download cancelled
101	User declined signature generation request
102	User requested to see changes in data on an error 74
103	User cancelled action
104	Get of file names cancelled by user
105	File deletions aborted
106	User not registered
107	Invalid user. The smartcard being used by this user isn't this user's card. If user never got prompted for card, have user properly register and try to re-enter CEFMS. If problem still occurs contact CEFMS support.
108	Same as 107, but with the SA card instead
109	CEFMS could not set expiration info on KTC for smartcard
110	CEFMS was unable to look up expiration info on KTC for smartcard. Note: this is almost *always* caused by firewall problems. Please make sure all firewalls involved have ports 2400-2407 open *both ways* between user's PC and CEFMS host.
128	Signature was created after originating user's card was deactivated
129	Signature was created after originating user's card was lost
130	Signature was created after originating SA's card was deactivated

131	Signature was created after originating SA’s card was lost
132	Signature was created after receiving user’s card was deactivated
133	Signature was created after receiving user’s card was lost
134	Signature was created after receiving SA’s card was deactivated
135	Signature was created after receiving SA’s card was lost
136	Smartcard is marked as lost at KTC
137	MAC on communications hash failed. Solution: re-try operation.
138	Signature was created before receiving SA’s card was activated
139	Signature was created before receiving user’s card was activated
140	Signature was created before originating SA’s card was activated
141	Signature was created before originating user’s card was activated
155	MAC on smartcard record at KTC failed
163	A attempt to verify a non-existent signature was made
167	User’s card has expired
168	SA’s card has expired
169	Signature was created after originating user’s card had expired
170	Signature was created after originating SA’s card was deactivated
200	Invalid MAC data was received by CEFMS from WinSig. Solution: re-try operation
225	The card in question is not marked as available on the KTC. Contact CEFMS support for investigation and resolution.
226	Smartcard already marked active on KTC. Have smartcard serial number and UID ready and contact CEFMS support for investigation.
227	Smartcard’s cryptoperiod has expired
228	User’s cryptoperiod has expired
229	SA’s cryptoperiod has expired
230	Originating user’s cryptoperiod has expired
231	Originating SA’s cryptoperiod has expired
234	Bad originating SA
235	Bad originating user
236	Bad receiving SA
237	Bad receiving user
238	Counter for this site does not exist on KTC
239	Counter for this site out of sync with KTC counter
242	Cannot open user database on KTC
243	KTC MAC on originating SA’s smartcard failed

244	KTC MAC on originating user's smartcard failed
245	KTC MAC on requesting SA's smartcard failed
247	Smartcard logging cancelled
248	KTC MAC on requesting user's smartcard failed
250	User already has an active smartcard at KTC. Contact CEFMS support with user's ID_NO for investigation.
251	A database-related error occurred internally in the CEFMS libraries. Please make sure you write down the *complete* error message that showed with this error, and contact CEFMS support for resolution.
251	Also can mean that the user's card hasn't been activated yet. If a 251 is received while the user is entering CEFMS or logging on with his card, it means the card isn't active. If a 251 comes at any other time, it's the previous definition. Yes, we goofed and gave two errors the same number.
252	SA's card hasn't been activated yet
255	Unknown command sent to WinSig. If user has a smartcard and got this error going into CEFMS, open WinSig configuration and make sure the esig package is enabled. WinSig will need to be restarted if anything is changed in configuration. If this doesn't resolve the problem, make sure user is properly registered.

APPENDIX A

SMARTCARD HOLDER'S RESPONSIBILITIES

APPENDIX A

SMARTCARD HOLDER'S RESPONSIBILITIES

If there are any questions concerning your responsibilities as a smartcard holder, please ask a District Security Officer (dSO) for an explanation. If there are no questions, sign and date this form; make a copy of the signed form for your records and return the original to the issuing dSO.

1. RECEIVING YOUR SMARTCARD.

   a. If a user appears in person to receive a smartcard:

      (1) A valid driver license or Civilian ID card may be required to verify identification.

      (2) The individual will be given a copy of the Electronic Signature Users Guide. The user must read, sign, and date the Smartcard Holders Responsibilities Form before receiving a smartcard and PIN. A copy of the signed signature page will be provided to the user.

      (3) After verifying the person's identity, the dSOs will activate the smartcard and issue the smartcard and PIN to the employee.

         - If the smartcard being issued is for a User, dSO1 will issue the smartcard and dSO2 will issue the User PIN envelope.

         - If the smartcard being issued is for a SA, dSO2 will issue the smartcard and dSO1 will issue the SA PIN envelope.

      (4) The individual will check the PIN envelope to detect tampering. If none is found, the user will sign the top portion of the envelope, tear it off, and return to the issuing dSO. The dSO will file the signed top portion.

      (5) The bottom portion containing the smartcard holder’s unique PIN (i.e., password) is kept by the individual.

   b. If a user is remotely located and cannot receive his/her card in person:

      (1) If the smartcard request is approved by the Smartcard Approver, the dSOs will assign a smartcard through the DSO CARD ASSIGNMENT SCREEN.

      (2) The requestor will be mailed the smartcard by **Certified Mail - Return Receipt Requested**.

(3) When you receive the smartcard, sign for the Certified Mail and call the issuing dSO to let him/her know you have received your smartcard. If you do not receive your smartcard in a reasonable amount of time or if the smartcard is damaged, notify the dSO so that appropriate action can be taken.

(4) Upon confirmation that you have the smartcard, the dSO will mail the PIN envelope by **Certified Mail - Return Receipt Requested**.

(5) When received, sign for the mail. Examine the PIN envelope for tampering. If okay, sign the top portion of the PIN envelope and tear it open. The bottom portion contains your PIN and serial number of your assigned card. **Memorize the PIN and destroy the bottom portion** of the envelope by shredding or burning. Any hard copy of a PIN must be kept in your physical possession or secured in a locked cabinet, drawer, or container accessible only by you.

(6) Return the top portion of the PIN envelope to the issuing dSO by **U.S. Postal Service - Regular Mail, First Class**.

(7) Call the issuing dSO to acknowledge receipt of the PIN envelope.

(8) Upon confirmation that you have received the PIN envelope, the appropriate dSO will activate the smartcard.

2. SMARTCARD and PIN USAGE. Your smartcard is logged on when entering CEFMS and logged off with a normal termination. **DO NOT LEAVE THE COMPUTER UNTIL YOU HAVE COMPLETED YOUR SESSION.**

   a. When exiting CEFMS, DO NOT remove your smartcard until you see the message "USER CARD IS BEING LOGGED OFF". Then you may remove your smartcard. If you remove your smartcard prior to this message, it will become locked.

   b. If your smartcard becomes locked, enter the CEFMS database again. A screen will prompt you to insert your smartcard and enter your PIN. If done properly, this procedure will unlock your smartcard, and allow you to successfully log into CEFMS.

3. SECURITY OF THE SMARTCARD AND PIN. Memorize your PIN. DO NOT write it down (especially on the smartcard) or share with others.

   a. When not in use, keep your smartcard in your possession, preferably a wallet or purse, or in a locked cabinet, drawer, or container accessible only by you. DO NOT LEAVE YOUR WALLET OR PURSE UNSECURED OR UNATTENDED BY YOU.

   b. If you retire, transfer, or leave the organization, you must notify the dSOs, return your smartcard to them for deactivation, and sign a Log Sheet for Deactivated Smartcards.

   c. Think of your smartcard as a personal credit card or blank check. The Electronic Signature generated by the smartcard is your signature. If another person uses it, you will bear the consequences.

4. SECURITY OF YOUR SMARTCARD AND PIN. A lost smartcard or compromised PIN is a serious security issue. You can be held responsible for transactions authorized with the missing or compromised card.

   a. If your PIN is revealed to someone else or you suspect it has been compromised, contact a dSO immediately for a new smartcard. Take the smartcard to the dSOs for deactivation and sign the Log Sheet for Deactivated Smartcards. Messages previously "signed" by you may still be verified.

   b. If your smartcard is lost/stolen, contact a dSO immediately for deactivation. You must go to the dSOs to obtain a new smartcard and PIN and sign a Log Sheet for Lost/Stolen Smartcards. Signatures generated by the lost/stolen smartcard after the deactivation date may not be verified.

5. SECURITY VIOLATIONS - WHAT SHOULD YOU REPORT? In addition to the above, report the following to the Security Office.

   a. If you see or know of unauthorized use of smartcards or PINs, i.e., sharing, notify the individual's supervisor for appropriate disciplinary action.

   b. If you find an unattended computer with a smartcard in the smartcard reader, attempt to log them off CEFMS and remove the smartcard. If you cannot log them off, remove the smartcard and take to the individual's supervisor. Inform the supervisor of the incident so that he/she may take appropriate disciplinary action.

c. If you find a smartcard, take it to your supervisor so he/she may decide if disciplinary action is necessary. The user may have already reported the loss of the smartcard to a dSO.

d. If you find a PIN written down, notify the supervisor for appropriate disciplinary action. PINs should be memorized and not written down for unauthorized viewing.

I certify that I have read and understand my responsibilities as a Smartcard Holder and that I am a Government employee.

_____	_____
PRINTED OR TYPED NAME	**SIGNATURE**

_____	_____	_____
OFFICE SYMBOL	**EXTENSION**	**DATE**

APPENDIX B

SMARTCARD APPROVERS DUTIES

APPENDIX B

SMARTCARD APPROVERS DUTIES

1. Each Corps of Engineers Financial Management System (CEFMS) site must appoint at least one Smartcard Approver. Smartcard Approvers will be appointed in writing and will be responsible for approving smartcard requests from Users and Security Administrators (SAs).

2. Smartcard Approvers will ensure the smartcard requestor is a Government employee. If in doubt, call the Security Office.

3. The Smartcard Approver must have a UNIX user ID and password and be given authority in the CEFMS Access Control Table to approve smartcard requests. Each Smartcard Approver must have a smartcard and PIN in order to electronically approve the requests.

4. A REQUEST FOR CEFMS ACCESS FORM must be completed for **each** employee requiring access to the CEFMS database. The forms will be submitted to the CEFMS DataBase Administrator. The CEFMS DBA will ensure the appropriate Smartcard Approver receives the names of individuals needing a smartcard.

5. Employees needing a smartcard will enter the CEFMS database and request a smartcard. The smartcard request will be forwarded electronically to the Smartcard Approver for action.

6. The Smartcard Approver must approve or disapprove the request. The APPROVE ELECTRONIC SIGNATURE SMARTCARD REQUEST SCREEN provides this capability. Access to this screen is limited to personnel designated as Smartcard Approvers.

    a. The APPROVE ELECTRONIC SIGNATURE SMARTCARD REQUEST screen displays all the smartcard requests that have not been approved or disapproved. The Smartcard Approver may use the arrow keys to scroll up and down through the pending requests. The cursor will automatically be positioned in the approved field for each pending request as they are scrolled.

    b. A request may be approved by entering "Y" or disapproved by entering "N" in the approved field.

c. If the Smartcard Approver desires, the <PgDn> key may be depressed to display detailed information about the request. To exit this screen, depress <Enter> to return to the original APPROVE/REJECT SMARTCARD REQUEST SCREEN.

d. When the Smartcard Approver is finished approving smartcard requests, depress the <End> key to commit the requests. If you depress the <F10> key, the screen will be exited and all approval actions will be discarded.

e. The approvals will be forwarded electronically to the dSOs who will issue the materials and PIN envelopes.

I certify that I have read and understand my responsibilities as a Smartcard Approver.

_____	_____
PRINTED OR TYPED NAME	**SIGNATURE**

_____	_____	_____
OFFICE SYMBOL	**EXTENSION**	**DATE**

APPENDIX C

DISTRICT SECURITY OFFICER (dSO)

OPERATING PROCEDURES

APPENDIX C

DISTRICT SECURITY OFFICER (DSO) OPERATING PROCEDURES

1. Designation of dSOs and Responsibilities.

   a. Each Corps of Engineers Financial Management System (CEFMS) site will have two primary dSOs designated dSO1 and dSO2 to perform Electronic Signature management functions for smartcards. DSO1 and dSO2 must have at least one backup (but no more than two) to perform their same functions. The backups are designated dSOb1 and dSOb2. **If a primary dSO and backup are both absent, Electronic Signature functions can not be performed.**

      (1) DSO1 (and dSOb1) will be responsible for the security and issuing of User smartcards and Security Administrator (SA) Personal Identification Number (PIN) envelopes.

      (2) DSO2 (and dSOb2) will be responsible for the security and issuing of SA smartcards and User PIN envelopes.

   b. Each dSO and backup will have a UNIX user ID and password and will be granted privileges by the CEFMS DataBase Administrator (DBA) to perform dSO functions. These functions will be set in the CEFMS Access Control Table.

   c. DSOs will be appointed in writing, must be government employees, and given training in the operating procedures and security requirements for Electronic Signatures before performing dSO functions.

   d. Smartcard Holders will be valid CEFMS users and have assigned authorization for electronic signature capability. DSOs will verify an individual's status before assigning, activating, or issuing a Smartcard. If unsure, dSOs will contact the Security Office.

Reference the dSO Manual for additional responsibilities and operating procedures.

APPENDIX D

OVERVIEW OF CARD ASSIGNMENT RULES

APPENDIX D

OVERVIEW OF CARD ASSIGNMENT RULES

Affected Card Types: User, SA, DSO and CSO

Users who are federal employees and US citizens may be assigned Esig cards. The only exception to the Federal Employee Requirement is where the site has written approval to issue a card to a non-US citizen or non-Federal employee by UFC, HQ, and GAO. Users should only be assigned one active user card from the home database.

Remote sites may assign access permissions on their database for users to perform Esig functions. The active Esig card assigned from the home database should be used to perform necessary functions on the remote database. Sites should not issue Esig cards to users who are not officially assigned to their database. The Esig card user is officially assigned to the home site database.

NOTE: If a user is temporarily reassigned to a remote site, the current Esig card issued from the home database should be used to perform Esig functions assigned to this user at the remote site.

If the user is temporarily reassigned to another site and does not currently have an Esig card assigned by the home database, he should input a request through the home database. Sites should never issue a card to a user who is not assigned to their site. If a user is not a Corps of Engineers employee, such as Audit employees, he should request a card as needed through Headquarters or the USACE Finance Center database. If a user permanently transfers to another site, the site he is leaving should deactivate the current card and the new home site should assign a new card as needed.

A user may be assigned an active User card and an active DSO card or an active CSO card. A user may be assigned an active SA card; however, no user can have an active SA and active User card simultaneously.

A user should not be assigned an active DSO and active CSO card. A user may not be assigned multiple active User, SA, active DSO or active CSO cards from any site or combination of sites that does not comply with the above restrictions.

NOTE: Cards should be deactivated when users become inactive on their home database. A user should never have an active card of any type if he is not an active employee on the home site/issuing site's database. Do not copy Esig card records across databases because it is unnecessary and causes system problems.